eSecurity

Treinamentos em Segurança da Informação

O que temos para hoje?

Menu do dia:

- ✓ **John the Ripper:**
  - ✓ Definição
  - ✓ Métodos
  - ✓ Opções de uso (--help)
  - ✓ Exemplos
  - ✓ Conhecendo Unshadow
  - ✓ Conhecendo o Johnny
  - ✓ Opções Avançadas

John the Ripper

John the Ripper é um software para quebra de senhas. Inicialmente desenvolvido para sistemas unix-like, corre agora em vários sistemas operativos (como DOS, Windows, Linux, BSD).

Disponível em versão livre e paga, o John the Ripper é capaz fazer força bruta em senhas cifradas em DES, MD4 e MD5 entre outras.

JtR: Métodos

O John the Ripper possui três modos de operação:

Dicionário (Wordlist): sendo o modo mais simples suportado pelo programa, este é o conhecido ataque de dicionário, que lê as palavras de um arquivo e verifica se são correspondentes entre si.

Quebra Simples (Single Crack): mais indicado para início de uma quebra e mais rápido que o wordlist, este modo usa técnicas de mangling e mais informações do usuário pelo nome completo e diretório /home em combinação, para achar a senha mais rapidamente.

Incremental: sendo o modo mais robusto no John the Ripper, ele tentará cada caractere possível até achar a senha correta, e por esse motivo é indicado o uso de parâmetros com o intuito de reduzir o tempo de quebra.

JtR: Métodos

Externo (External): o modo mais complexo do programa que faz a quebra a partir de regras definidas em programação no arquivo de configuração do programa, que irá pré-processar as funções no arquivo no ato da quebra quando usar o programa na linha de comando e executá-las. Este modo é mais completo e necessita de tempo para aprender e acostumar-se.

Fonte: Wiki

JtR: Opções

Veja algumas opções do John the Ripper:

–single: Define o modo “single” para quebrar as senhas.

–wordlist=ARQUIVO: Define o modo “wordlist” para quebrar as senhas e define o arquivo ARQUIVO como sendo de onde as senhas serão lidas. Aqui você pode utilizar também a opção –stdin para dizer que as palavras virão da entrada padrão.

–incremental: Define que será utilizado o modo “incremental” para quebrar a senhas. Opcionalmente você pode definir que tipo de modo incremental será utilizado fazendo –incremental[=MODO].

–external=MODO: Define que será utilizado o modo external.

–rules: Habilita as regras para wordlist definidas em john.conf quando se utiliza o modo wordlist.

JtR: Opções

–stdout[=LENGTH]: Quando utilizado, faz com que o JtR imprima as possíveis senhas direto na saída padrão ao invés de tentá-las contra um hash. Se você definir o parâmetro LENGTH só serão impressas senhas com caracteres até a quantidade especificada em LENGTH.

–restore[=NOME]: Faz com que uma sessão que foi interrompida anteriormente continue de onde parou. Se você definir um nome diferente para a sessão, especifique o nome dela na linha de comando junto com esta opção. A sessão fica gravada na home do John, em um arquivo chamado john.rec.

–session=NOME: Define o nome da sessão que pode ser utilizado com a opção restore. A esse nome será automaticamente adicionado a extensão .rec.

–status[=NOME]: Mostra o status da última sessão ou, se definido o nome da sessão, da sessão especificada.

–make-charset=ARQ: Gera um arquivo charset para ser utilizado no modo "incremental".

JtR: Opções

–show: Mostra as senhas do arquivo que você especificou para o JtR que já foram quebradas. Esta opção é especialmente útil quando você tem outra instância do JtR rodando.

–test: Esta opção faz um benchmark de todos os algoritmos compilados no software e os testa para saber se estão funcionando corretamente. Esta opção já foi explicada anteriormente.

–users=[-]: Nome do usuário ou UID: Com esta opção você pode especificar para o JtR quais usuário você quer tentar quebrar a senha. Você pode utilizar o nome de usuário ou o UID dele e pode separar vários usuários utilizando uma vírgula. Utilizando o “-” antes do nome do usuário, você faz com que o John ignore aquele usuário ou UID.

–groups=[-]GID: Faz com que o John tente quebrar apenas as senhas dos usuários participantes de um grupo especificado (ou ignorá-los, se você utilizar o “-”).

JtR: Opções

–shells=[-]SHELL: Apenas tenta quebrar as senhas dos usuários cujas shells sejam iguais à que foi especificada por você na linha de comando. Utilizando o “-” você ignora as shells especificadas.

–salts=[-]NUMERO: Deixa você especificar o tamanho das senhas que serão (ou não) testadas. Aumenta um pouco a performance para quebrar algumas senhas, porém o tempo total utilizando esta opção acaba sendo o mesmo.

–format=FORMATO: Permite a você definir o algoritmo a ser usado para quebrar a senha, ignorando a detecção automática do software. Os formatos suportados atualmente são DES, BSDI, MD5, AFS e LM. Você também pode utilizar esta opção quando estiver utilizando o comando –test, como já foi explicado anteriormente neste texto.

–save-memory=1, 2 ou 3: Esta opção define alguns níveis para dizer ao John com qual nível de otimização ele irá utilizar a memória. Os níveis variam de 1 a 3, sendo 1 a mínima otimização. Esta opção faz com que o JtR não afete muito os outros programas utilizando muita memória

JtR: Exemplos

Podemos realizar ataques utilizando a opção single crack
john --single hashes.txt

Podemos também fazer ataques híbridos com o comando abaixo:
john --wordlist="wordlist.txt" –rules hashes.txt

Além dos ataques anteriores, podemos testar o incremental:
john --incremental="alnum" hashes.txt

Perceba que utilizamos a opção alnum, assim como no crunch, para que ele trabalhe de modo alfanumérico.

Quando você não define um modo de ataque, ele seguirá a sequência acima, ou seja, irá testar primeiro o Single Crack, depois baseado em Wordlist e por ultimo o Incremental.

JtR: Conhecendo Unshadow

O script unshadow é parte integrante do John the Ripper e tem o objetivo de mixar os arquivos passwd e shadow para que o JtR faça a quebra utilizando os métodos anteriores.

Para conseguir acesso ao Shadow, só se tornando root do Sistema Operacional ou ter a maravilhosa sorte de conseguir o backup desse arquivo de alguma maneira.

Para utilizar o unshadow, utilize o seguinte comando:

```
unshadow /etc/passwd  /etc/shadow  >  senhas.txt
```

Como o tempo é algo precioso, podemos especificar no nosso arquivo senhas.txt os usuários que estamos interessados:

```
john --users=root senhas.txt
john --users=root,joao senhas.txt
```

Ou dizer os usuários que não queremos:

```
john --users=-joao  senhas.txt
```

JtR: Conhecendo o Johnny

Johnny é um GUI (uma interface gráfica) para o John the Ripper. Desenvolvido por "Shinnok.s", esta versão inclui as principais funcionalidades da ferramenta em um belo painel.

O raciocínio por trás Johnny é simples, mas ao mesmo tempo profundo: a complexidade através da simplicidade.

Johnny é escrito em C++ utilizando o framework Qt, tornando-se multi-plataforma: Unix/Linux e sistemas operacionais Windows.

Ele foi programado como parte do Google Summer of Code 2012, e suporta arquiteturas 32-bits e 64-bits.

A interface também deixa espaço para muitas novas opções, como, detecção de hash, edição de dicionário, geração de charsets interativos e bruteforce, criação de regras e muito mais.

JtR: Opções Avançadas

Definindo um formato de senha:

```
john --show --format=DES --single senhas.txt
```

Podemos solicitar o John que gere as senhas de modo incremental e depois nos envie essa sequencia de senhas em tela através da sintaxe stdout com um limite máximo de caracteres.

```
john --incremental  --stdout=8
```

É possível criar uma sessão durante a quebra de senhas e depois migrar ou continuar essa sessão posteriormente:

```
john --sesion=gravando senha.txt
```

Depois podemos restaurar de onde paramos:

```
john --restore=gravando
```

Definindo um formato de senha:

```
john --show --format=DES --single senhas.txt
```

JtR: Opções Avançadas

As regras do John, no Kali, estão disponíveis no arquivo:
/etc/john/john.conf

Podemos também trabalhar com Prefixos conhecidos com o sinal ^ e o Sufixo, definido no john the ripper pelo sinal $.

Suponhamos que estamos suspeitando que a senha tenha os caracteres 2014, podemos utilizar os sufixos e prefixos da seguinte maneira:
O JtR irá procurar na senha essa opção, no formato que ela se encontra, seja no começo da senha, no meio ou no fim.
^[2]^[0]^[1]^[4]

O exemplo abaixo, irá fazer com que ele trabalhe pseudo aleatorioamente entre as senhas:
$[4]$[1]$[2] $[0]

Ou podemos trabalhar com ranges
$[1-9]$[1-9]$[1-9]$[1-9] e ^[1-9]^[1-9]^[1-9]^[1-9]

Chega por hoje

www.eSecurity.com.br

E-mail: alan.sanches@esecurity.com.br

Twitter: @esecuritybr e @desafiohacker

Skype: desafiohacker

Fanpage: www.facebook.com/academiahacker